IN THE CIRCUIT COURT OF JACKSON COUNTY, MISSOURI
AT KANSAS CITY

ALEXANDRIA STOBBE, individually and on behalf of all others similarly situated, **Plaintiff,** **vs.** **ROCKHURST UNIVERSITY, a Missouri Corporation,** **[Serve: CT Corporation System** **120 South Central Avenue** **Clayton, MO 63105]** **Defendant.**	**Case No.:** **Division:**

CLASS ACTION PETITION FOR DAMAGES

COMES NOW Plaintiff Alexandria Stobbe ("Plaintiff"), individually and on behalf of all others similarly situated, and for her Petition against Defendant Rockhurst University ("Rockhurst" or "Defendant"), respectfully states and alleges as follows:

NATURE OF THE CASE

1. This is a class action brought by Plaintiff, individually and on behalf of all others similarly situated (*i.e.*, the Class Members), seeking to redress Defendant's intentional, willful and reckless violations of their privacy rights. Plaintiff and the other Class Members are faculty, staff and/or are student employees of Rockhurst University who entrusted their personally identifiable information ("PII") to Defendant. Defendant betrayed Plaintiff's trust by failing to properly safeguard and protect their PII and publicly disclosing their PII without authorization in violation of Missouri common law.

2. This action pertains to Defendant's April 2016, unauthorized disclosure of employee IRS W-2 forms to a third party (the "Data Breach"), during which Plaintiff's and the

EXHIBIT B

other Class Members' PII was stolen and disseminated to unauthorized persons as a direct and/or proximate result of Defendant's failure to safeguard and protect their PII.

3. The wrongfully disclosed PII included, *inter alia*, Plaintiff's and the other Class Members' names, mailing addresses, salary amounts, withholding amounts, and Social Security numbers.

4. Defendant flagrantly disregarded Plaintiff's and the other Class Members' privacy and property rights by intentionally, willfully and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized disclosure. Plaintiff's and the other Class Members' PII was improperly handled, inadequately protected, readily able to be copied by data thieves and not kept in accordance with basic security protocols. Defendant's obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiff's and the other Class Members' rights, both as to privacy and property.

5. Plaintiff has standing to bring this action because as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff has incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy and/or (ii) the additional damages set forth in detail below, which are incorporated herein by reference.

6. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market. For example, stolen PII is sold on the cyber black market for $14 to $25 per record to (i) individuals needing or wanting a new identity or healthcare, or focused on committing fraud, (ii)

medical service providers, medical device manufacturers and drug manufacturers for targeted marketing and advertising campaigns for their products and services, and (iii) health insurers for targeted marketing and advertising campaigns for their health insurance products and to monitor their insureds' medical conditions for purposes of adjusting their health insurance premiums.

7. Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiff's and the other Class Members' PII and not yet used the information will do so at a later date or re-sell it.

8. Accordingly, Plaintiff and the other Class Members seek redress against Defendant for breach of implied contract, invasion of privacy by the public disclosure of private facts, common law negligence and bailment.

9. Plaintiff, on behalf of herself and the other Class Members, seeks (i) actual damages, economic damages, and/or nominal damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, and costs.

JURISDICTION AND VENUE

10. The Court has jurisdiction over the parties and the subject matter of this action. Jurisdiction is proper because both Plaintiff and Defendant are residents of the State of Missouri and Defendant is a business operating, and licensed under, the laws of the state of Missouri.

11. Venue is proper in Jackson County, Missouri, pursuant to RSMo §508.010 because the acts complained of occurred and Defendant is located in the City of Kansas City, Missouri.

PARTIES

12. Plaintiff Alexandria Stobbe is a citizen of Missouri and resides in Jackson County, Missouri. Plaintiff is an employee of Rockhurst University and, as a result, entered into an implied contract with Defendant for the adequate protection of her PII. Plaintiff had her PII exposed as a result of Defendant's inadequate safety and security protocols governing PII.

13. Rockhurst University is a Missouri not-for-profit corporation with its headquarters in Kansas City, Missouri.

BACKGROUND FACTS

14. Certain allegations are made upon information and belief.

15. As a part of its business operations, Defendant Rockhurst collects and maintains PII of its employees.

16. On or about April 4, 2016, Defendant disclosed employee IRS W-2 forms to an unauthorized third party (the "Data Breach"), during which Plaintiff's and the other Class Members' PII was stolen and disseminated to unauthorized persons.

17. The wrongfully disclosed PII included, *inter alia*, Plaintiff's and the other Class Members' names, mailing addresses, salary amounts, withholding amounts, and Social Security numbers.

18. Upon information and belief, the Data Breach affected an estimated 1200 of Defendant's employees.

19. As a direct and/or proximate result of Defendant's failure to properly safeguard and protect the PII of its employees, Plaintiff's and the other Class Members' PII was stolen, wrongfully disseminated without authorization and compromised.

20. On or about April 13, 2016, the President of Rockhurst University informed "Rockhurst Faculty, Staff and Student Employees" of the Data Breach and indicated the University was arranging "identity theft and credit monitoring protection for all affected employees free of charge."

21. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, the criminal(s) and/or their customers now have Plaintiff's and the other Class Members' compromised PII. There is a robust international market for the purloined PII. Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud[1] and medical fraud.

22. Identity theft occurs when someone uses an individual's PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* Federal Trade Commission, Fighting Back against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/ about-identity-theft.html (last

[1] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

visited Jan. 18, 2013). The Federal Trade Commission estimates that the identities of as many as nine million Americans are stolen each year. *Id.*

23. The Federal Trade Commission correctly sets forth that "Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit." *Id.*

24. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim's information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also have been known to give a victim's PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

25. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[2] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to

[2] *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 (http://www.ftc.gov/os/2012/03/120326privacyreport.pdf).

combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[3]

26. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified that their PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

27. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html). Thus, a person whose PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

28. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a

[3] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35-38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12.

fresh start. For some victims of identity theft, a new number may actually create new problems; because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

29. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. "Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits." *Id.*

30. The Data Breach substantially increased Plaintiff's and the other Class Members' risk of being victimized by "phishing." "Phishing" is an attempt to acquire information (and sometimes, indirectly, money), such as usernames, passwords and credit card details by masquerading as a trustworthy entity through an electronic communication. *See* http://www.onguardonline.gov/articles/0003-phishing (last visited Jan. 18, 2013).

31. Communications purporting to be from popular social websites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and often directs users to enter details at a fake website that looks and feels almost identical to the legitimate one. When criminals have access to PII from a large group of similarly situated victims, it is much more

feasible to develop a believable phishing spoof email. They can then get this group of victims to reveal additional private information, such as credit cards, bank accounts, and the like.

32. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiff's and the other Class Members' prior written consent to disclose their PII to any other person—as required by laws, regulations, industry standards and/or internal company standards.

33. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's and the other Class Members' PII to unauthorized persons.

34. Upon information and belief, Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by failing to keep or maintain an accurate accounting of the PII wrongfully disclosed in the Data Breach.

35. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and the other Class Members' PII to protect against anticipated threats to the security or integrity of such information. Defendant's unwillingness or inability to establish and maintain the proper information security procedures and controls is an abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

36. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy rights, and harmed them in the process, by depriving Plaintiff and the other Class Members of the value of their PII, for which there is a well-established national and international market. *See, e.g.*, T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

37. Aside from the criminal element, frequent purchasers of purloined PII include other data thieves and fraudsters, pharmacies, drug manufacturers, medical device manufacturers, hospitals and insurance companies, who use the information to market their products and services directly to the data breach victims and/or to adjust the victims' medical insurance premiums. *Id*. Plaintiff and the other Class Members, not data thieves, should have the right to sell their PII and receive the corresponding financial benefits.

38. The actual harm and adverse effects to Plaintiff and the other Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's above wrongful actions and/or inaction and the resulting Data Breach requires Plaintiff and the other Class Members to take affirmative acts to recover their peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts—for which there is a financial and temporal cost.

Plaintiff and the other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

39. Victims and potential victims of identity theft, identity fraud and/or medical fraud—such as Plaintiff and the other Class Members—typically spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from data breaches. *See Defend: Recover from Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html; *Fight Identity Theft*, www.fightidentitytheft.com. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of $1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. *Id*. at 6.

40. Other statistical analyses are in accord. The GAO found that identity thieves use PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PII, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

41. Defendant's wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the other Class Members' PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of

Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical fraud, (iii) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Data Breach risk mitigation products, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Data Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze, (v) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Data Breach, and/or (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market.

CLASS ACTION ALLEGATIONS

42. Pursuant to Rule 52.08 of the Missouri Rules of Civil Procedure, Plaintiff brings this class action as a class action on behalf of herself and the following Class of similarly situated individuals:

> **All persons who were employed by Defendant and whose names, mailing addresses, salary amounts, withholding amounts, and/or Social Security numbers contained in the employees W-2 forms were disclosed by Defendant.**

43. On information and belief, the putative Class is comprised of approximately 1200 employees making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

44. The rights of Plaintiff and each other Class Member were violated in a virtually identical manner as a direct and/or proximate result of Defendant's willful, reckless and/or negligent actions and/or inaction and the resulting Data Breach.

45. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Defendant willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the other Class Members' PII;

b) Whether Defendant was negligent in failing to properly safeguard and protect Plaintiff's and the other Class Members' PII;

c) Whether Defendant owed a duty to Plaintiff and the other Class Members to exercise reasonable care in safeguarding and protecting their PII;

d) Whether Defendant breached its duty to exercise reasonable care in failing to safeguard and protect Plaintiff's and the other Class Members' PII;

e) Whether Defendant was negligent in failing to safeguard and protect Plaintiff's and the other Class Members' PII;

f) Whether, by publicly disclosing Plaintiff's and the other Class Members' PII without authorization, Defendant invaded their privacy; and

g) Whether Plaintiff and the other Class Members sustained damages as a result of Defendant's failure to safeguard and protect their PII.

46. Plaintiff and her counsel will fairly and adequately represent the interests of the other Class Members. Plaintiff has no interests antagonistic to, or in conflict with, the other Class Members' interests. Plaintiff's lawyers are highly experienced in the prosecution of consumer class action and data breach cases.

47. Plaintiff's claims are typical of the other Class Members' claims in that Plaintiff's claims and the other Class Members' claims all arise from Defendant's failure to properly safeguard and protect their PII.

48. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and the other Class Members' claims. Plaintiff and the other Class Members have been harmed as a result of Defendant's wrongful actions and/or inaction and the resulting Data Breach. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct.

49. Class certification, therefore, is appropriate pursuant to Missouri Rule 52.08(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

50. Class certification also is appropriate pursuant to Missouri Rule 52.08(b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

51. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action, Defendant will retain the benefits of its wrongdoing despite its serious violations of the law.

COUNT I

BREACH OF IMPLIED CONTRACT

52. The preceding factual statements and allegations are incorporated herein by reference.

53. Plaintiff and the other members of the Class, as part of their employment agreement with Defendant, provided Defendant their PII.

54. In providing such PII, Plaintiff and the other members of the Class entered into an implied contract with Defendant, whereby Defendant became obligated to reasonably safeguard

Plaintiff's and the other Class members' PII.

55. Under the implied contract, Defendant was obligated to not only safeguard the PII, but also to provide Plaintiff and Class members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

56. Defendant breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their PII.

57. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure of their PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and (vii) deprivation of the value of their PII, for which there is a well-established national and international market—for which they are entitled to compensation. At the very least, Plaintiff and Class members are entitled to nominal damages.

COUNT II

NEGLIGENCE

58. The preceding factual statements and allegations are incorporated herein by reference.

59. Defendant owed a duty to Plaintiff and the other Class Members to safeguard and protect their PII.

60. Defendant breached its duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the other Class Members' PII.

61. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PII would result in an unauthorized third party gaining access to such information for no lawful purpose.

62. Plaintiff and the other Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendant's failure to secure and protect their PII in the form of, *inter alia*, expenses for adequate credit monitoring and identity theft insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit freeze, loss of privacy, deprivation of the value of their PII, and other economic and non-economic harm (as detailed above), for which they are entitled to compensation.

63. Defendant's wrongful actions and/or inaction and the resulting Data Breach (as described above) constituted (and continue to constitute) negligence at common law.

COUNT III

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

64. The preceding factual statements and allegations are incorporated herein by reference.

65. Plaintiff's and the other Class Members' PII was (and continues to be) sensitive and personal private information.

66. By virtue of Defendant's failure to safeguard and protect Plaintiff's and the other Class Members' PII and the resulting Data Breach, Defendant wrongfully disseminated Plaintiff's and the other Class Members' PII to unauthorized persons.

67. Dissemination of Plaintiff's and the other Class Members' PII is not of a legitimate public concern; publicity of their PII was, is and will continue to be offensive to

Plaintiff, the other Class Members and all reasonable people. The unlawful disclosure of same violates public mores.

68. Plaintiff and the other Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendant's invasion of their privacy by publicly disclosing their private facts (*i.e.*, their PII) in the form of, *inter alia*, expenses for adequate credit monitoring and identity theft insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit freeze, loss of privacy, deprivation of the value of their PII, and other economic and non-economic harm (as detailed above), for which they are entitled to compensation. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

69. Defendant's wrongful actions and/or inaction and the resulting Data Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PII) without their authorization or consent.

COUNT IV

BAILMENT

70. The preceding factual statements and allegations are incorporated herein by reference.

71. Plaintiff and the other Class Members entrusted their PII to Defendant as part of their business relationship with Defendant. Plaintiff and the other Class Members were entitled to trust that their PII in Defendant's possession would likewise be properly protected from unlawful access.

72. Plaintiff's and the other Class Members' PII is their personal property. Defendant's wrongful actions and/or inaction and the resulting Data Breach deprived them of the value of their PII, for which there is a well-established national and international market, because the PII is now in the hands of unauthorized person(s) and compromised.

73. During the time of bailment, Defendant owed Plaintiff and the other Class Members the duty to safeguard and protect their PII by maintaining reasonable and effective data security practices, procedures and protocols to protect their PII. As alleged herein, Defendant breached its duty to Plaintiff and the other Class Members by failing to safeguard and protect their PII which, in turn, directly and/or proximately caused the Data Breach and the wrongful dissemination of their PII to unauthorized persons.

74. Defendant's breach of this duty directly and/or proximately caused Plaintiff and the other Class Members to suffer (and continue to suffer) the injuries and damages alleged herein.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative and appointing Plaintiff's counsel as Lead Counsel for the Class;

B. declaring that Defendant breached its implied contract with Plaintiff and Class members;

C. declaring that Defendant negligently disclosed Plaintiff's and the Class members PII;

D. declaring that Defendant has invaded Plaintiff's and Class members' privacy;

E. Ordering Defendant to pay actual damages to Plaintiff and the other members of the Class;

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class members;

G. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff;

H. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

I. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiff, on behalf of herself and the other Class Members, respectfully demands a trial by jury on all of his claims and causes of action so triable.

Respectfully submitted,

/s/Mitchell L. Burgess

BURGESS LAW FIRM, P.C.
Mitchell L. Burgess, Mo. Bar # 47524
1000 Broadway, Suite 400
Kansas City, MO 64105
(816) 471-1700
(816) 471-1701 FAX
mitch@burgesslawkc.com

THE NORMAN LAW FIRM LLC
Phyllis A. Norman, Mo. Bar #55887
1000 Broadway, 4th Floor
Kansas City, MO 64105
(816) 288-9622
(816) 471-1701
phyllis@pnormanlaw.com

RALPH K. PHALEN, ATTORNEY AT LAW
Ralph K. Phalen, Mo. Bar #36687
1000 Broadway, Suite 400
Kansas City, Mo. 64105
(816) 589-0753
(816) 471-1701 FAX
phalenlaw@yahoo.com

ATTORNEYS FOR PLAINTIFF